CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Seagate Secure ® TCG SSC Self-Encrypting Drives (CPP FDE EE V2.0E)

Maintenance Report Number: CCEVS-VR-VID10857-2020-2

Date of Activity: 20 July 2020

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." March 20, 2013

Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements" Version 1, February 2004

Seagate Secure ® TCG SSC Self-Encrypting Drives Impact Analysis Report #7 Version 1.0 June 10, 2020

Seagate Secure ® TCG SSC Self-Encrypting Drives Security Target Version 8.0, Proprietary June 10, 2020

Seagate Secure ® TCG SSC Self-Encrypting Drives Security Target Version 8.0, Public June 10, 2020

Seagate Secure® TCG Enterprise SSC Self-Encrypting Drive and TCG Opal SSC Self-Encrypting Drive Common Criteria Full Drive Encryption – Encryption Engine Key Management Description, Version 8.0 June 10, 2020

Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 8.0 June 10, 2020

Affected Evidence:

Seagate Secure ® TCG SSC Self-Encrypting Drives Security Target Version 8.0, Proprietary June 10, 2020

Seagate Secure ® TCG SSC Self-Encrypting Drives Security Target Version 8.0, Public June 10, 2020

Updated Developer Evidence:

Code change did not have any impact on the developer evidence of the validated TOE.

Description of ASE Changes:

Seagate Technology, LLC. submitted an Impact Analysis Report (IAR #7) to CCEVS for approval to update the code in four Common Criteria certified Seagate product models; ST10000NM010G, ST12000NM008G, ST14000NM012G, and ST16000NM009G; and for approval to add one new version of firmware, EF03, based on existing Common Criteria certified version revision EF02.

Code changes to the firmware were to improve performance and reliability, to correct spec violations, and status reporting errors. Code changes also fixes bugs in command timeout, drive hang, incorrect error reporting, and logging errors. These code changes did not impact the crypto software and, therefore, did not require update to the CAVP certificates. There were no changes to the EAR except to add the new firmware version.

Changes to TOE:

Firmware version EF03 is based on existing Common Criteria certified version revision EF02. The hardware models use the firmware versions as shown in the following table.

Validated Hardware Versions	New Firmware Versions
ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	EF03

Description of ALC Changes:

Changes to the following documents were made, going from version 7.0 to 8.0:

- Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 8.0 Proprietary June 10, 2020
- Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 8.0 Public June 10, 2020
- Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 8.0 Dated: June 10, 2020

- Seagate Secure® TCG Enterprise SSC Self-Encrypting Drive and TCG Opal SSC Self-Encrypting Drive Common Criteria Full Drive Encryption – Encryption Engine Key Management Description Report Version 8.0 Dated: June 10, 2020

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR #7) for the four Common Criteria certified models listed above
- The IAR specifies that there are no security relevant firmware changes
- There are a relatively small number of changes to the validated TOE, and none of the changes impact the secure operation of the TOE. The assurance impact of these changes is minor. There are no changes to the development environment.
- Code change did not have any impact on the developer evidence of the validated TOE.
- The changes to the ST and other documents were limited to document version with the addition of the new firmware version.

Description of Regression Testing:

For all storage products, Seagate performs a lengthy and rigorous suite of regression tests before releasing any firmware revisions. Regression testing performs a comprehensive set of security and non-security related test cases, including tests for device I/O throughput and performance, device read/write verification, servo performance, shock and vibration, environmental, secure port locking, firmware updates, secure boot signature verification and roll back protection. In addition, secure SED and FIPS or CC certified secure storage products are tested for all aspects of security including all TCG commands, ATA commands, FDE encryption modes, credentials, retry limits, band creation and deletion, and FIPS and CC mode testing. The entire regression test process takes about 3 weeks to complete. Regression testing was conducted for these firmware releases starting April 10, 2020 and ending May 4, 2020.

Vulnerability Assessment:

Seagate searched 3 vulnerability databases, National Vulnerability Database (NVD, https://nvd.nist.gov/), MITRE Common Vulnerabilities and Exposures (CVE, http://cve.mitre.org/cve/), and United States Computer Emergency Readiness Team (US-CERT, http://www.kb.cert.org/vuls/html/search) for a large number of terms, on May 19, 2020. No new vulnerabilities were found.

Vendor Conclusion:

The 'Description of Changes' section (Chapter 2) of this IAR indicates that there are no changes to the development environment of the validated TOE. The 'Description of Changes' section of this IAR further indicates that there to the product associated with the validated TOE. Of these, none are security relevant.

Based on this and other information from within this IAR document, the assurance impact of these changes is minor.

Validation Team Conclusion:

The validation team reviewed the changes and concur the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The updated Security Target, the Entropy Document, and the Key Management Description were only changed to add the new firmware version identified above. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.